Volume 01 October 2008

This Issue

New DigiCert Customers

Sony
House of Representatives
Hewlett Packard
Verizon
Stanford University
Cisco

New DigiCert Customer Account Area:

As featured in the 'Upcoming Items' section of last month's newsletter, DigiCert has unveiled a new customer account area.

This design refresh makes it easier to locate certificates, make changes to the account settings, create and redeem Purchase Orders, buy certificates, and become a reseller.

The update was the final step in the plan to bring DigiCert's latest offerings full swing to its customers. The customer account area was also updated to prepare for our new Managed PKI, which is in development. More information about this can be found on page 2.

digicert®
Your Success is Built on Trust™

Strong Value in Troubled Times

"DigiCert Saved Us $298,000"

At what point do we begin making compromises on the things we shouldn't have to? With a volatile economy, accelerating inflation rates, and increases in the cost of everyday living, one has to stop and ponder the meaning of value.

This was a concern of a certain DigiCert client. Through the years we've developed a great relationship with him, but we were still astounded when he told us they have saved nearly $300,000 in costs associated with SSL certificates since they switched to DigiCert.

He calculated the cost of individual certificates from his previous provider, and factored in how much it would have cost to implement the same security solution provided by DigiCert. The result is that their organization has spent only a few thousand for our wildcard certificates as opposed to the hundreds ouf thousands that would have been necessary to secure the same names.

Since they weren't willing to spend that much before, their organization simply used to measure the risks and forgo SSL security on items they thought were less likely to be targets of attack.

DigiCert to the rescue. With our WildCard certificate solution, this valued customer has been able to apply SSL certificates whenever, wherever, and however he needs for a fraction of the cost of our competitors.

DigiCert is driven to provide the best value for SSL certificates. We have developed innovative features that allow our certificates to be more flexible, more compatible, and easier to use.

We include free reissues for the lifetime of a certificate, 24-hour support (with no hold lines for that matter), and many of our certificates enjoy an unlimited server license.

We're glad we can help our customers meet security needs without compromising their budgets.

Call us toll free (Canada or US) at 1-800-896-7973 (International Customers please call us at +1-801-877-2100). Visit us online at www.digicert.com (24-hour Live Chat service provided).

WildCard Certificates

Unlimited names, servers, and possiblities

Wildcard certificates can be used to secure an unlimited number of subdomains of a given base domain. For example, a wildcard certificate for *.example.com can be used to secure mail.example.com, admin.example.com, test.example.com, etc.

DigiCert's WildCard Plus pioneered the use of a common SSL feature -- Subject Alternative Names (SANs) -- to create uncommon flexibility and compatibility in two ways: 1) A certificate issued to *.example.com will include a SAN for "example.com," which do not secure the base domain itself; and 2) DigiCert allows you to list SANs you want included in the certificate, appeasing mobile platforms that choke on the * character in the common name.

These features, along with DigiCert's Unlimited Server License, will enable you to cover every facet of your domain, something most organizations simply cannot afford the time or money to do.

Learn More About WildCard Certificates

Industry Issues

The Truth About Server Gated Cryptography (SGC)

By: Christopher Skarda, VP of Operations

When customers ask us why we don't offer SGC certificates, our answer is simple: Because less than 1% of the browser market requires SGC certificates, SGC certificates are effectively obsolete. And because those browsers are extremely outdated and vulnerable to malicious attacks, SGC certificates actually promote *in*security, which is the opposite of what we want to provide.

Server Gated Cryptography (SGC) certificates were created in response to a United States federal legislation limiting the export of software capable of supporting strong (128-bit) encryption.

Internet browsers in the late 1990's were designed to limit SSL encryption strength to weak (40-bit) encryption unless the site was secured using an SGC Certificate, which would enable these browsers to use strong encryption. SGC Certificates were only distributed to financial institutions.

In 2000, the US Government lifted the export ban of strong cryptography. As a result, SGC became available to all types of organizations and browsers began supporting strong encryption for all certificates.

"SGC certificates condone the use of outdated browsers, giving the end user a false sense of security."

Shortly after the ban lift, many browsers were still in use that required an SGC certificate to establish strong encryption. Because of this, many server administrators chose to purchase SGC certificates to ensure that all of their visitors could connect with 128-bit encryption.

Today, these outdated browsers -- less than 1% of the market -- are no longer supported by their developers, even for known security vulnerabilities, making them vulnerable to viruses and malware such as key loggers. SGC certificates condone the use of outdated browsers, giving the end user a false sense of security.

A better solution is to use a non-SGC certificate, then configure your webserver to require strong encryption for your site. This will help to limit the number of outdated browsers that connect to your site, thus reducing your liability and protecting your clients.

Upcoming Items

Managed PKI for Enterprise Accounts

By: Jeff J. Snider, Director of Web Development

In late October, DigiCert will launch its new enterprise-level Managed PKI service, which will allow organizations to have complete control over the management of their digital certificates, including real-time issuance, reissues and replacements, renewals, and revocations.

Organizations using the new M-PKI system will enjoy all the benefits offered with standard DigiCert services – top-notch support, strong encryption and compatibility, and terrific value – along with the ability to perform key life-cycle events on demand.

With Managed PKI, DigiCert will perform the validation on domains and organizations ahead of time so that certificates can be issued immediately whenever they are needed. In this way, DigiCert maintains its high standards of validation, and clients are able to bypass the typical one-hour waiting period for their certificates.

If you would like to be notified when DigiCert's Managed PKI service launches, please go to http://www.digicert.com/managed-pki-ssl.htm or email mpki@digicert.com.

Value of Chained Certificates:

By: Dan Egbert, Web Developer

Security-conscious Certificate Authorities, like DigiCert, use chained certificates to provide the greatest level of security and protection.

Chained SSL certificates use an intermediate to link between the primary certificate and trusted root.

This makes it easy to issue certificates that are trusted in all major browsers. Using chained certificates gives the greatest possible security for Certificate Authorities and their customers.

If a root certificate is compromised, all of the certificates issued by it lose their value. Using Intermediate certificates allows a Certificate Authority to lock away a root certificate so there is no possibility that it could be compromised while signing other certificates.

This additional level of security may be why the vast majority of Certificate Authorities utilize intermediate certificates.

All major servers support intermediate certificates and are automatically installed on Microsoft IIS and Exchange servers.

DigiCert, Inc.
355 South 520 West
Canopy Building II
Lindon, UT 84042
+1-800-896-7973 ph
+1-866-842-0223 fax
www.digicert.com

Feedback? Article Suggestions? We want to know! Send an email to newsletter@digicert.com